Exhibit 31

Excerpts of SW-SEC00012332

ENTERPRISE INFORMATION SECURITY GUIDELINES

Version 1.4

November 8, 2017

Information Technology

5. SERVER HARDENING

5.1. Server operating systems must be an official SolarWinds licensed and supported version.

5.2. Appropriate vendor supplied security patches and firmware updates must be applied.

5.3. Unnecessary software, system services, protocols, ports, and drivers must be removed.

5.4. Servers must be configured with enterprise managed anti-virus, anti-malware software, and a host based firewall. Exceptions shall be granted on a case by case basis.

5.5. Local system accounts and credentials should not be used. The default administrator account should be renamed. Guest accounts should be renamed and disabled. Do not allow auto-login and ensure that a session timeout is configured to log a user out after a defined period of time in accordance with the access control guidelines.

5.6. Appropriate local file system/sharing permissions, local/physical security, reporting, intrusion detection, and logging/auditing must be enabled.

5.7. Appropriate Domain-based Active Directory server based group policies must be enforced. Exceptions shall be granted on a case by case basis.

5.8. Post-Install operating system, utility/system service patches, database, web, and application security patches shall be pre-tested and deployed on a regular basis against similar systems before rolling out to the production environment.

5.9. Periodic audits of server compliance shall be conducted at least annually. Results shall be documented and any deficiencies corrected.

6. IN HOUSE APPLICATIONS THAT ACCESS, MANAGE OR STORE DATA

6.1. Access Control and Domain authentication.

6.2. Privileged access controlled especially for databases/data stores.

6.3. IT audit and monitoring enabled.

6.4. Data classified as moderate or higher should be encrypted or anonymized if possible

6.5. If unable to encrypt or anonymize data, a need to know model should be enabled and increased audit frequency and inspection of access should be completed.

6.6. Passwords cannot contain the user's account name or parts of the user's full name that exceed two consecutive characters.

6.6.1. Passwords must be at least 8 characters in length.

6.6.2. Passwords must contain characters from three of the following four categories:

6.6.3. English uppercase characters (A through Z).

6.6.4. English lowercase characters (a through z).

6.6.5. Base 10 digits (0 through 9).

6.6.6. Non-alphabetic characters (for example, !, $, #, %).

VERSION CONTROL

Version	Date	Author	Description/Revision
1.0	9/26/17	T.Brown	Development of GDPR Access Guidelines
1.2	9/28/17	T. Brown	Deprecated policy and changed to guidelines. Added logging, auditing, and hardening requirements
1.2	10/3/17	K.Pierce	Revised formatting and added differences between v1.0 and 1.2
1.3	10/17/2017	T.Brown	Added Secure Delete
1.4	11/8/2017	E. Quitugua	Provided clarification around password requirements
1.4.1	11/8/2017	R.Johnson	Updated 9. Product Development Requirements based on SDL Updated 12. Data Classification with FISMA matrix

